HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
APO 09128-4209

DIRECTIVE
NUMBER 55-9

25 APR 1996

OPERATIONS

Operations Security

1. **Summary**. To promulgate policy and guidance on maintenance of Operations Security (OPSEC) within USEUCOM.

2. **Applicability**. Applies to the United State European Command and all of its components.

3. **Internal Control Systems**. This Directive contains internal control provisions and is subject to the requirements of the internal management control program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. **Suggested Improvements**. Users can send suggestions for improving this directive to Headquarters European Command, Operations Directorate, ECJ33, Unit 30400 Box 1000, APO AE 09128.

5. **References**.

*a. JCS SM 362-84: Joint Operation Planning System, VOL I, as amended by USEUCOM Supplement 1 (UNCLASSIFIED).

*b. JCS SM 142-85: Joint Operation Planning System, VOL II, as amended by USEUCOM Supplement 1 (SECRET).

c. JCS PUB 18: Policy, Concept, and Standards for Operations Security (CONFIDENTIAL).

d. JCS document: OPSEC Survey Guide (CONFIDENTIAL).

6. **Explanation of Terms**. See Appendix A.

7. **General**.

a. A force has an advantage when it can surprise the enemy. To do this, that force must protect its operations and activities through sound security practices. The purpose of OPSEC is to protect military operations and activities by denying indicators of friendly plans, intentions, and capabilities to enemy intelligence collectors. This involves preventing the enemy from determining what, where, when, and how friendly operations will occur, until it is too late for enemy forces to effectively react to those operations.

b. OPSEC is the responsibility of commanders and chiefs of security assistance organizations (SAO), and requires support from staffs at all echelons. The intelligence staff provides enemy threat data, the support staff identifies possible friendly indicators of activity or intention, and the operations staff recommends OPSEC measures. The commander determines what OPSEC measures will be implemented and the time frame for their implementation, or what level of risk he is willing to accept.

c. OPSEC does not supersede or replace the traditional security programs (physical security, information security, and communications security) which are oriented toward protecting classified information within reasonably well defined spheres of functional responsibility. OPSEC complements those programs by addressing indicators of operational intent and capability.

8. **Policy**. Achievement of surprise is essential to military effectiveness and requires continuous

This Directive supersedes ED 55-9, dated 6 Jun 1986.

protection of capabilities and intentions. Application of OPSEC is the principal means of achieving that protection.

a. OPSEC is a command responsibility. As such, OPSEC considerations will be identified and applied at all command levels for military operations, exercises, and activities which, if unprotected, could reveal sensitive operational capabilities, weapon system capabilities, plans, and/or procedures.

b. Development and distribution of preliminary OSPEC guidance will coincide with preparation of the planning directive, command planning guidance, or planning for theater introduction of new/improved weapon systems.

c. OPSEC considerations will be identified and applied by responsible individuals from each respective area of functional responsibility (e.g., operations, plans, intelligence, logistics, communications, public affairs, and personnel).

d. OPSEC training programs will be established at HQ USEUCOM, and within each component command to develop and maintain an optimal level of OPSEC knowledge among all members of assigned military forces and the DOD civilian work force.

9. **Procedures**.

a. An essential feature of OPSEC is the identification of those aspects of an operation which require protection. Each office responsible for developing or supporting an operational plan or action is also responsible for ensuring that sensitive elements of information relating to that plan or action are identified and that timely distribution of guidance relating to their protection is made to appropriate personnel. Categories of information requiring protection are referred to as essential elements of friendly information (EEFI). The EEFI relate to specific aspects of an operation or activity that must be withheld from a potential enemy. The EEFI may themselves be classified or unclassified or a combination of both and include, for example, operational intentions, capabilities, timing, weaknesses, or procedures. The time-phased protection of EEFI will normally correlate to the planning, preparation, execution, and post-operation phases of an operation or activity. EEFI describe what information must be protected and the duration of protection.

b. An enemy or potential enemy must rely on detectable activities associated with an operation as principal indicators concerning that operation. Indicators may take the form of press releases, pre-positioning of combat forces, sudden increases in message traffic volume, ordering of logistics buildups, etc. Such indicators may not necessarily be EEFI, but could reveal exploitable information sufficient to compromise an operation. Planners must consider the potential indicators that may be exploited from planning direction issued on an operational activity and, in coordination with the operations officer responsible for the plan or action, develop appropriate OPSEC measures.

c. EEFI and indicators must be identified as early as possible during the planning process. Dissemination of EEFI will be accomplished as per guidance contained in references to this directive. In those instances where guidance does not exist, EEFI may be distributed by message or letter, as appropriate, using format guidance, to the extent possible, offered by references b and c.

10. **Responsibilities**.

a. HQ USEUCOM.

(1) The Chief of Staff will chair a HQ USEUCOM OPSEC Advisory Board, consisting of the Directors of Manpower, Personnel and Administration; Intelligence; Operations; Logistics and Security Assistance; Plans & Policy; Command, Control, and Communications Systems; Public Affairs; and the Chief, Data Services Center. The Inspector General and the Chief, National Security Agency/ Central Security Service, Europe (NCEUR), will serve as associate members. Selected

representatives from other activities may be invited to attend advisory board meetings by members or associate members. Attendance by non-members will be coordinated with the Director, J3. The board will meet semi-annually, or as directed by the chairman, to:

(a) Provide command guidance for achieving JCS and HQ USEUCOM OPSEC objectives.

(b) Develop OPSEC policy applicable to USEUCOM.

(c) Review OPSEC surveys/ operation security evaluations (OSE) conducted or recommended by HQ USEUCOM. (Ref Appendix C)

(d) Provide command review and direction to the USEUCOM OPSEC program.

(2) A representative of J3 will chair an OPSEC Working Group consisting of representatives from the Directorates of Manpower, Personnel and Administration; Intelligence, Logistics and Security Assistance; Plans & Policy, Command, Control, and Communications Systems; Public Affairs; the Data Services Center; and NCEUR. The Working Group will oversee OPSEC matters on a continuing basis. It will meet quarterly, or as directed by the chairman, to:

(a) Identify and pursue headquarters initiatives on OPSEC.

(b) Identify proposed candidates for OPSEC surveys/ evaluations.

(c) Provide stimulation and coordination to the HQ USEUCOM OPSEC program.

(d) Address OPSEC problems referred to it by the OPSEC Advisory Board, the Director of Operations, and members.

(3) The Director of Operations, J3:

(a) Has primary responsibility for the command OPSEC program.

(b) Designates an officer as the single point-of-contact for OPSEC matters within the Headquarters and to chair the OPSEC Working Group.

(c) Ensures that OPSEC training materials are provided to HQ USEUCOM staff elements and SAO for familiarizing all personnel with the vulnerability of U.S. forces to hostile observation and exploitation.

(d) Directs accomplishment of OPSEC surveys/OSEs and preparation of reports, as appropriate.

(e) Maintains liaison with other agencies, activities, and commands for the purpose of exchanging OPSEC items of interest.

(f) Submits annual OPSEC program reports, as of 30 Jun. to arrive at the office of the Joint Chiefs of Staff by 1 Sep.

(g) Maintains an OPSEC briefing and provides briefings as required.

(h) Is responsible for the administration of the HQ USEUCOM OPSEC Advisory Board.

(i) Serves as the U.S. representative to SHAPE on all in theater OPSEC matters as directed by JCS.

(j) Develops, reviews, or approves OPSEC annexes for USCINCEUR plans, as appropriate.

(4) The Director of Intelligence, J2:

(a) Disseminates hostile OPSEC threat information and intelligence to the staff, appropriate commands, and SAO.

(b) Maintains a briefing on the hostile threat as it relates to OPSEC and provides briefings, as required.

(5) The Director of Command, Control, and Communications Systems, C3S:

(a) Manages COMSEC programs and operations in USEUCOM and exercises staff supervision over COMSEC monitoring and analysis activities initiated in support of USEUCOM OPSEC program.

(b) Provides advice and assistance regarding National and Theater COMSEC directives and their application to OPSEC.

(c) Provides briefings on COMSEC/ELSEC capabilities and limitations, as required.

(d) Evaluates COMSEC support of joint operations and exercises to determine the effectiveness of COMSEC planning and actions which can/should be taken to correct COMSEC weaknesses and, therefore, improve force OPSEC posture.

(e) Initiates and promulgates instructions for joint COMSEC improvement in support of OPSEC goals/objectives.

(f) Acts as Executive Agent for management of designated USEUCOM COMSEC surveillance missions.

(g) Determines and coordinates USEUCOM joint and combined communications security equipment and material requirements, including joint and combined tactical force requirements, in support of OPSEC surveys.

(h) Includes COMSEC material, equipment, and surveillance requirements in USEUCOM operations and exercise plans and reviews component command supporting plans to ensure that adequate COMSEC support requirements are identified and programmed.

(i) In support of OPSEC, promotes the exchange of COMSEC information and procedures among theater commands and COMSEC activities.

(j) Identifies anticipated fiscal year communications security surveillance requirements involving component command support of joint activities.

(k) Acts as primary liaison with ECJ3 for matters relating to COMSEC support and communications-oriented cryptographic material in support of the USEUCOM OPSEC program.

(6) All Directors:

(a) Comply with OPSEC policy as stated herein.

(b) Develop OPSEC annexes/guidance for plans or activities over which primary staff responsibility is held, and contribute OPSEC guidance to plans/ activities for which collateral responsibility is held.

(c) Support OPSEC surveys/OSEs as required.

(d) Appoint an OPSEC officer to be responsible for directorate OPSEC matters and identify that individual's name to ECJ3.

(e) Provide newly assigned personnel (military and civilian) with an OPSEC awareness orientation within 60 days of arrival and with OPSEC reorientation training annually.

b. CINCUSAREUR, CINCUSNAVEUR, and CINCUSAFE:

(1) Comply with OPSEC policies established by this and service directives. Conflicts between this and service directives will be identified to HQ USEUCOM, ECJ33.

(2) Establish training programs to ensure that all personnel are familiar with OPSEC considerations and applications.

(3) Establish and pursue component-oriented OPSEC objectives.

(4) Provide guidance and assistance to subordinate organizations during the preparation of operations/contingency/exercise plans to ensure optimum consideration of OPSEC.

(5) Conduct OPSEC surveys/ evaluations in accordance with this and service directives.

(6) Submit OSPEC Quicklook Reports, when appropriate, in accordance with this directive. (Ref; Appendix B)

(7) Establish a command OPSEC Board, under the cognizance of the operational staff with representation from major staff agencies, to:

(a) Assess the command status of

OSPEC.

(b) Review results of OPSEC surveys.

(c) Determine operations to be examined by OPSEC surveys/ evaluations.

(8) Designate an officer within the operations staff to be the focal point for OPSEC. This officer should have a TOP SECRET security clearance and access to SI.

(9) Provide an annual message report on the status of the component command OPSEC program to USCINCEUR, ATTN: ECJ33. The report will reflect status as of 30 Jun and arrive at this HQ NLT 31 Jul. The report will contain the following data:

(a) Overview of OPSEC program status.

(b) Training/indoctrination program activities.

(c) OPSEC surveys conducted during the reporting period, to include a summary of survey findings.

(d) Problem areas and recommendations.

(e) Lessons learned.

(f) Component command OPSEC objectives.

(g) Forecast of OPSEC activities for next reporting period.

(10) Forward one copy of command directives implementing OPSEC to USCINCEUR, ATTN: ECJ33.

c. USEUCOM Security Assistance Organizations will:

(1) Comply with OPSEC policies established by this directive.

(2) Establish and administer a training program to ensure that all personnel are familiar with OPSEC considerations and applications.

(3) Conduct periodic OPSEC evaluation/reviews of activities.

(4) Submit OPSEC Quicklook Reports, when appropriate, in accordance with this directive.

(5) Designate an officer to be the focal point for OPSEC.

FOR THE COMMANDER IN CHIEF:

RICHARD F. KELLER
Lieutenant General, USA
Chief Of Staff

OFFICIAL:

W. L. Kiser
SUSAN M. MEYER
LTC, USA
Adjutant General

DISTRIBUTION:
P

Appendixes

A - Definitions
B - OPSEC Quicklook Reporting
C - Operations Security Survey

Appendix A

Explanation of Terms

A-1. **Operations Security (OPSEC)**. The protection of military operations and activities resulting from the identification and subsequent elimination or control of intelligence indicators susceptible to hostile exploitation.

A-2. **Operations Security (OPSEC) Data Base**. A narrative and graphic identification of all events associated with planning and executing an operation or function, including documentation of all known enemy efforts to obtain prior knowledge or foreknowledge of an operation or types of operations.

A-3. **Command, Control and Communications Countermeasures (C3CM)**. The integrated use of operations security (OPSEC), military deception, jamming, and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary C3 capabilities, and to protect friendly C3 against such actions.

A-4. **Deception**. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests or to cause injurious delay in his decisions and operations.

A-5. **Physical Security**. That element of security which results from all physical measures necessary to safeguard classified equipment, material, and documents from access or observation by unauthorized persons.

A-6. **Information Security**. A system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order or statute.

A-7. **Communications Security (COMSEC)**. The protection resulting from the application of cryptosecurity, transmission security, and emission security measures to telecommunications and from application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value which might be derived from the possession and study of such telecommunications or to ensure the authenticity of such telecommunications.

A-8. **Electronics Security (ELSEC)**. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the interception and study of noncommunications electromagnetic radiations (e.g., radar).

A-9. **Signals Security (SIGSEC)**. A generic term which includes both COMSEC and ELSEC.

A-10. **OPSEC Survey**. A methodology used to determine the degree of protection afforded to a given operation or function, characterized by multiple functional outlines to identify all possible sources of information disclosure. Appendix III of this Directive provides expanded discussion of the survey.

A-11. **Operations Security Evaluation (OSE)**. An alternate survey methodology tailored to individual security-sensitive organization requirements where the organization is vulnerable to the all-source hostile threat and requires a sophisticated but focused threat assessment and/or vulnerability analysis.

Appendix A
(Cont)

Explanation of Terms

A-12. **Essential Elements of Friendly Information (EEFI)**. Aspects of information relating to planning, to an operation, or to a weapon system requiring protection. EEFI may take the form of questions or the form of positive statements. In either case, an EEFI listing should identify the duration of required protection and identify from whom the information should be protected. References b and c provide expanded guidance on EEFI development.

Appendix B

OPSEC Quicklook Reporting

B-1. **Discussion**. Personnel who have been adequately trained in OPSEC doctrine and application will be able to detect procedures detrimental to unit OPSEC posture as a matter of routine. This function should automatically take place in normal daily activities and operations, during special or atypical operations, and in the course of reviews and assessments of operations in which the unit has been previously engaged. If an OPSEC vulnerability is detected, a Quicklook Report is encouraged to alert others to problems identified. Procedures detrimental to OPSEC detected during a special operation or exercise for which a post exercise report is already required should include these OPSEC deficiencies as part of the report. OPSEC Quicklook reporting affords individual commands the opportunity to review their OPSEC posture using organic resources, and provides lessons learned to other military commanders. By definition, OPSEC Quicklook Reports are entirely voluntary; however, their submission should be encouraged by all commanders. Quicklook Reports provide a means of improving military operational effectiveness based on the experience of other commanders. Reports should be given widest distribution via the operational chain of command to ensure broadest application to military operations.

B-2. **Report Format**. OPSEC Quicklook Reports should contain the following types of information:

a. Explanation of the problem(s) identified.

b. Evaluation of the promulgated EEFI, if any. (Were they specific and comprehensive enough to alert personnel to the sensitive aspects of the operation? Were personnel familiar with them?)

c. Evaluation of operational guidance. Was it based on EEFI and a knowledge of the hostile threat? Was it helpful in avoiding disclosure of sensitive information?

d. Recommendations for further developing/refining EEFI.

e. Recommendations for changes to operational guidance and countermeasures such as procedural/tactical changes, equipment modifications, and OPSEC initiatives to reduce or eliminate the problem(s).

B-3. **Report Distribution**. Quicklook Resorts should be distributed via the operational chain of command within component commands of USEUCOM. Component command headquarters will forward copies of Quicklook Reports warranting intercomponent attention to HQ USEUCOM/EcJ3-oD, and other component command headquarters as appropriate.

B-4. **Utility**. An OPSEC Quicklook Report, or a series of similiar Quicklook Reports, may point out an especially significant, persistent, or widespread deficiency in the OPSEC measures which are being applied to a particular operation or activity. Additionally, there may be indications that an enemy or potential enemy is exploiting certain unknown OPSEC weaknesses which are rendering an operation or mission unsuccessful, compromising the results of an R&D project, or disclosing intentions, capabilities, and tactics during the course of an exercise. If such is the case, an OPSEC survey may be in order.

Appendix C

Operations Security Survey

C-1. **Discussion**. Operations Security (OPSEC) surveys offer one method for evaluating the adequacy of security measures applied to a specific operation or task. Such surveys are normally conducted by teams composed of representatives from the various functional staff elements that may be participating in the operation or task. Reference d provides guidance on planning the accomplishment of an OPSEC survey. The following paragraph, with its subparagraphs, broadly defines an OPSEC survey and identifies functional aspects of the survey. Findings of OPSEC surveys are intended for use by commanders in improving the operational security and, consequently, the effectiveness of their commands.

C-2. **OPSEC Survey**. A methodology used to determine the degree of protection afforded to a given operation or function, characterized by multiple functional outlines to identify all possible sources of information disclosure. Functional outlines include:

a. Communications. An identification of who talks to whom, what is transmitted, how the transmission is made, and when it occurs in relation to the planning and execution of an operation.

b. COMSEC. An identification of all COMSEC measures and material available for a given operation, system, or organization and a determination of the amount and type of use of those measures and materials.

c. Electromagnetic. An identification of electromagnetic emitters associated with an operation and function, including their deployment, probable emission patterns, and times of activation in relation to significant events of an operation or function.

d. ELSEC. An identification of all ELSEC measures and material available for a given operation or system, and a determination of the amount and type of use of those measures and materials.

e. **Intelligence Threat**. An identification of all known and possible enemy capabilities to collect and exploit information from a given or similar operation. This threat would include known enemy intelligence collection and analysis capabilities, efforts, and successes. An integral part of these data is an assessment of enemy human intelligence, and reconnaissance satellite capabilities.

f. **Operations**. An identification of all entities participating in an operation, their actions, and the time those actions occur in planning and executing an operation or function It also includes identification of procedures used in the conduct and support of operations to ascertain whether stereotyped, predictable procedures are employed.

g. **Physical Security**. An assessment of all physical security measures taken to safeguard classified equipment, material, and documents from access or observation by unauthorized persons.

h. **Supplementary Data**. An identification of support function relating to or supporting operations (e.g., logistics, personnel, administration, etc.).

C-3. **Reporting**. Reference d (Annex H) contains the suggested OPSEC survey reporting format.